UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

ASHLEY DIXON, individually, and on behalf of all others similarly situated**,** Plaintiff, v. **M&D CAPITAL PREMIER BILLING LLC, and ISLAND AMBULATORY SURGERY CENTER LLC,** **Defendants.**	**Case No.** CLASS ACTION JURY DEMAND

CLASS ACTION COMPLAINT

Plaintiff, Ashley Dixon brings this Class Action Complaint, against Defendants, M&D Capital Billing LLC ("M&D") and Island Ambulatory Surgery Center LLC ("Island Ambulatory") (collectively, "Defendants"), and each of their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, members, and/or other related entities, and upon personal knowledge as to her own actions, and information and belief as to all other matters, allege as follows:

INTRODUCTION

1. This action arises out of the public exposure of the confidential, private information of Defendant's current and former patients, Personally Identifying Information[1] ("PII") and

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendants, not every type of information included in that definition was compromised in the Data Breach.

Protected Health Information ("PHI")[2] (collectively "Personal Information"), including of Plaintiff and the Class Members, which was in the possession of Defendants in a cyberattack on M&D's systems, beginning on or around June 20, 2023, caused by Defendants' collective failures to adequately safeguard that Personal Information ("the Data Breach").

2. According to Defendants, the Personal Information unauthorizedly disclosed in the Data Breach includes patients' name, address, medical billing and insurance information, certain medical information such as diagnosis, medication and treatments, and demographic information such as date of birth, Social Security number, and financial information.[3]

3. M&D, a healthcare advisory firm, provides services such as, physician, facility, and non-par provider hospital billing, professional coding, claims recovery, review of billing practices, and credentialing.[4]

---

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. A "covered entity" is further defined as, *inter alia*, a group health plan. *Id. Covered entity, Health plan*. A "business associate" is defined as, with respect to a covered entity, a person who: "creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA], including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management and repricing…" *Id. Business associate*. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, Dep't for Health & Hum. Servs., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 5, 2022). Island Ambulatory is clearly a "covered entity," and M&D is clearly a "business associate," subject to HIPAA, and some of the PHI compromised in the Data Breach is "protected health information," subject to HIPAA.

[3] Notice of Data Breach ("Notice") attached hereto as **Exhibit A**.

[4] https://mdcapitalbilling.com/services/ (last accessed Mar. 28, 2024)

4. Island Ambulatory is a surgery and recovery center[5].

5. Defendants failed to undertake adequate measures to safeguard the Personal Information of Plaintiff and the proposed Class Members.

6. Although Defendants purportedly discovered the Data Breach on July 8, 2023, they failed to immediately notify and warn current and former patients, with M&D waiting until March 21, 2024 to provide written notice to Plaintiff and the proposed Class.[6]

7. As a direct and proximate result of Defendants' failures to protect current and former patients' sensitive Personal Information and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class Members have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

PARTIES

8. Plaintiff, Ashley Dixon is a natural person and resident and citizen of New York, where she intends to remain. Plaintiff Dixon is a former patient of Island Ambulatory Surgery Center, LLC, and a Data Breach victim.

9. Defendant M&D is a Limited Liability Company organized and existing under the laws of the State of New York with a principal place of business at 115-06 Myrtle Avenue, Richmond Hill, New York 11418.

10. Defendant Island Ambulatory is a Limited Liability Company organized and existing under the laws of the State of New York with a principal place of business at 2279 Coney Island Avenue, Brooklyn, New York 11223.

[5] http://www.islandasc.com/ (last accessed Mar. 28, 2024)
[6] Exhibit A

JURISDICTION & VENUE

11. This Court has original jurisdiction over this action under the Class Action Fairness Act 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

12. This Court has personal jurisdiction over Defendants because they each are organized and exist under New York law and do substantial business in New York.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because M&D's principal place of business is in this District and a substantial art of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND FACTS

A. Defendants M&D and Island Ambulatory

14. According to Defendant M&D's Website[7]:

> M&D Capital is much more than a medical billing service: we are a business partner that can help you manage a significant portion of your operations, proactively and efficiently.
>
> We are a specialty healthcare advisory firm that assists healthcare providers to grow their businesses. Our principals have deep experience in managing complicated financial affairs of medical practices. We believe that every viable medical practice has the potential for growth. We specialize in helping practices with financial challenges realize significant gains in revenue.

15. According to Defendant Island Ambulatory's Website[8]:

> Island Ambulatory Surgery Center's mission is to bring together many specialists who are committed to providing the highest quality of care in the safest environment possible. From the moment you are admitted to the center through surgery and recovery, you will find our dedicated staff is here to address your concerns, answer all your questions and provide you with an exceptional experience. We deliver accommodating, compassionate safe surgical care of the

[7] https://mdcapitalbilling.com/about-us/ (last accessed Mar. 28, 2024)
[8] http://www.islandasc.com/ (last accessed Mar. 28, 2024)

> highest quality, guided by local ownership and control, for the greater convenience, improved medical outcomes and increased satisfaction of our patients.

16. On information and belief, M&D is a service provider of Island Ambulatory performing medical billing for Island Ambulatory and was provided with Plaintiff's and the proposed Class Members' Personal Information.

17. Island Ambulatory requires that its patients provide it with their Personal Information, which Island Ambulatory provides to M&D in connection with M&D performing these services.

18. M&D collects and stores Plaintiff's and the proposed Class Members' Personal Information on its information technology computer systems, on information and belief in New York, including but not limited to their name, address, medical billing and insurance information, certain medical information such as diagnosis, medication and treatments, and demographic information such as date of birth, Social Security number, and financial information.

19. When Defendants collect this Personal Information, they promise to use reasonable care to protect and safeguard the Personal Information, from unauthorized disclosure.

20. On information and belief, Island Ambulatory maintains a Notice of Privacy Practices in which it states that, "…we are committed to protecting the privacy of your medical information," and acknowledges that:

> [W]e are required by law to:
> - Maintain the confidentiality of your medical information
> - Provide you with this notice of our legal duties and privacy practices concerning medical information.
> - Follow the terms of our notice of privacy practices in effect at the time[9].

[9] http://www.islandasc.com/patients-rights-responsibilities-at-island-ambulatory-surgery-center/notice-of-privacy-practices/ (last accessed Mar. 28, 2024)

21. On information and belief, Island Ambulatory maintained an identical or substantially similar policy prior to the Data Breach.

22. Therein it states that Island Ambulatory may disclose Personal Information as needed to "treat you, to seek payment for services, and to conduct day-to-day operations.[10]

23. None of the purposes for which Defendants may disclose patient Personal Information without authorization include the Data Breach which came to pass.

24. Island Ambulatory represented to its patients that it would take adequately measures to safeguard their Personal Information, including ensuring that its business associate, M&D, undertook adequate measures to safeguard that Personal Information, and Plaintiff and members of the proposed Class relied on Island Ambulatory's representations when they agreed to provide their Personal Information to Island Ambulatory.

25. Despite their alleged commitments to securing sensitive patient data, Defendants do not follow industry standard practices in securing patients' Personal Information and failed to protect the Personal Information of Plaintiff and the proposed Class Members from unauthorized disclosure in the Data Breach.

B. Defendants M&D and Island Ambulatory Fail to Safeguard Personal Information—the Data Breach

26. On information and belief, according to Defendants, beginning on or around June 20, 2023 M&D experienced a cyberattack to its computer information technology systems by an "unauthorized threat actor," which from that time until July 8, 2023 resulted in the unauthorized disclosure and exfiltration of patients' Personal Information, including of Plaintiff and the proposed Class Members, including name, address, medical billing and insurance information,

[10] *Id*.

certain medical information such as diagnosis, medication and treatments, and demographic information such as date of birth, Social Security number, and financial information—the Data Breach.[11]

27. Nevertheless, Defendants waited over ***eight*** (8) months to inform affected current and former patients of the unauthorized disclosure of their Personal Dara Breach in the Data Breach, waiting until March 2024 for M&D to provide written notice to Plaintiff and the Class.

28. On or about March 21, 2024, M&D began sending written notice of the Data Breach to affected current and former patients, including Plaintiff, and the proposed Class Members.[12]

2. The Data Breach Notice stated:

> On or around July 8, 2023, we identified suspicious activity within our computer environment. We immediately took steps to secure our network and launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. Through the investigation, we determined that an unauthorized threat actor may have had access to certain systems beginning on or around June 20, 2023. As a result, certain files within our systems may have been accessed or acquired by the unauthorized threat actor. Based on the investigation we determined that your data may have been included on the impacted systems.
>
> **What information was Involved?**
>
> The impacted systems contained demographic and healthcare information provided by the Covered Entity, which may include your name, address, medical billing and insurance information, certain medical information such as diagnosis, medication and treatments, and demographic information such as date of birth, Social Security number and financial information.[13]

29. In addition, in its Data Breach Notice, M&D recommended that affected persons "remain vigilant and continually review your healthcare insurance information. Additionally, you should continually review your credit report, bank account activity and bank statements for

[11] Exhibit A.
[12] *Id*.
[13] *Id*.

irregularities…" and offered them complimentary credit monitoring through Equifax for one (1) year.[14]

30. The M&D Data Breach Notice did not further elaborate on the nature or extent of the Data Breach, omitting its scope or size.

31. Defendants' conduct, by acts of commission or omission, caused the Data Breach, including: M&D's failures to implement best practices and comply with industry standards concerning computer system security to adequately safeguard patient Personal Information, allowing Personal Information to be accessed and stolen, and by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach, and by failing to adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems, resulting in the Data Breach; as well as Island Ambulatory's failure to ensure their business associate, M&D, undertook these data security measures and appropriate employee training, prior to Island Ambulatory providing M&D with Plaintiff's and the Class Members' PHI.

32. On information and belief, as more fully articulated below, Plaintiff and the members of the proposed Class Members' Personal Information, was unauthorizedly disclosed to, and actually "exfiltrated by," third-party cybercriminals in the Data Breach, has now or will imminently be posted to the Dark Web for public viewing and use, in the public domain, and/or utilized for criminal and fraudulent purposes and misuse.

[14] *Id*.

C. Plaintiff's Experience

33. Plaintiff, Ashley Dixon, is a former patient of Island Ambulatory, who received treatment from Island Ambulatory.

34. Island Ambulatory utilized M&D for medical billing services.

35. As a condition of receiving Island Ambulatory's medical services, Plaintiff was required to provide her Personal Information to Island Ambulatory, which Island Ambulatory then provided to M&D in connection with M&D's medical billing services, including but not limited to Plaintiff's name, address, medical billing and insurance information, certain medical information such as diagnosis, medication and treatments, and demographic information such as date of birth, Social Security number, and financial information.

36. Plaintiff typically takes measures to protect her Personal Information and is very careful about sharing her Personal Information. Plaintiff has never knowingly transmitted Personal Information over the internet or other unsecured source.

37. Plaintiff stores any documents containing her Personal Information in a safe and secure location, and she diligently chooses unique usernames for her passwords and online accounts.

38. In entrusting her Personal Information to Defendants, Plaintiff believed that, as part of the payments for medical treatment and services, Defendants Island Ambulatory and M&D would adequately safeguard that information. Had Plaintiff known that M&D did not utilize reasonable data security measures, and that Island Ambulatory did not ensure M&D utilized reasonable data security measures, Plaintiff would not have entrusted her Personal Information to said Defendants or would have paid less for those treatments and services.

39. Plaintiff received M&D's Data Breach Notice dated March 21, 2024, informing her that her Personal Information, including her name, address, medical billing and insurance information, certain medical information such as diagnosis, medication and treatments, and demographic information such as date of birth, Social Security number, and financial information, was impacted and exfiltrated in the Data Breach, if on file for her.[15]

40. As a direct and proximate result of the Data Breach permitted to occur by Defendants, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Personal Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be used for criminal, fraudulent purposes and/or has been sold for such purposes and posted on the dark web for sale; Plaintiff has been and will be forced to expend considerable time and effort to monitor her accounts and credit files, changing her online account passwords, verifying the legitimacy of Defendant's Data Breach Notice and researching the Data Breach, to protect herself from identity theft and fraudulent misuse of her Personal Information, disclosed as a result of the Data Breach.

41. In addition, as a result of the Data Breach, Plaintiff also suffered diminution in the value of her Personal Information, a form of intangible property that she entrusted to Island Ambulatory and M&D for the sole purpose of obtaining medical services.

42. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of her Personal Information in the Data Breach.

43. She fears for her personal financial security and uncertainty over the information disclosed in the Data Breach, and is experiencing emotional distress over the unauthorized disclosure of her Personal Information. She is experiencing feelings of anxiety, embarrassment,

[15] Exhibit A.

sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

44. Plaintiff was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive Personal Information and the harm caused by the Data Breach. She was also outraged that Defendants took months to notify her of the Data Breach even as it was discovered in July 2023.

45. As a result of the Data Breach, Plaintiff faces a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like her Social Security Number and date of birth.

46. Furthermore, Plaintiff's sensitive Personal Information remains in Defendants' possession without adequate protection against known threats, exposing Plaintiff to the prospect of additional harm.

C. This Data Breach was Foreseeable by Defendants.

47. Plaintiff and the proposed Class Members provided their Personal Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

48. By failing to do so, Defendants put Plaintiff and Class Members at risk of identity theft, financial fraud, and other harms.

49. Defendants tortiously, or in breach of their implied contracts, failed to take the necessary precautions required to safeguard and protect the Personal Information of Plaintiff and the Class Members from unauthorized disclosure. Defendants' actions represent a flagrant

disregard of Plaintiff's and the other Class Members' rights.

50. Plaintiff and Class Members were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing Personal Information and the critical importance of providing adequate security for that information.

51. According to a Chief Strategy Officer at ClearDATA, "[i]t's no secret that healthcare is the industry most plagued by data breaches. Patient data is the most valuable, making it targeted by bad actors."[16]

52. Moreover, healthcare companies are targeted because of their cybersecurity vulnerabilities: "…healthcare is also targeted because it is very vulnerable. Many healthcare providers use outdated IT infrastructure and operating systems that can no longer be patched or supported, such as Windows 7 and Windows Server 2008, even after Microsoft retired them. Further, more than half of medical devices operate on legacy systems, and 83% of medical imaging devices are on outdated operating systems that no longer receive patches/updates. This creates significant cybersecurity vulnerabilities and makes it much easier for bad actors to find an entry point into the network." [17]

53. Cyber-attacks against healthcare organizations such as Defendants are targeted and frequent. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal

[16] Sanjay Cherian, Forbes Magazine, "Healthcare Data: The Perfect Storm," January 14, 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=28523ee56c88 (last accessed. June 19, 2023).
[17] *Id*.

experience in U.S. healthcare organizations with many of the incidents initiated by bad actors…"[18]

54. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[19]

55. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[20]

56. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[21]

57. According to the ITRC's January 2023 report for 2022, "[t]he number of publicly reported data compromises in the U.S. totaled 1,802 in 2022. This represents the second highest number of data events in a single year and just 60 events short of matching 2021's all-time high number of data compromises."[22] In 2022, there were approximately 422 million individuals affected by cyberattacks.[23]

---

[18] HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, *2019 HIMSS Cybersecurity Survey*, available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last accessed December 7, 2022)

[19] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 7, 2022)

[20] *Ibid.*

[21] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last accessed Apr. 14, 2023).

[22] Identity Theft Resource Center, 2022 Data Breach Report, available at https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, pg. 7 (last accessed Jul. 3, 2023).

[23] *See Id.*, pg. 2.

58. Moreover, of the 1,802 data breaches in 2022, ITRC reported that 1,560 involved compromised names, 1,143 involved compromised of Social Security Numbers, and 633 involved compromised dates of birth—types of PHI included in the unauthorized disclosure in this Data Breach.[24]

59. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[25]

60. Furthermore, Defendants were aware of the risk of data breaches because such breaches have dominated the headlines in recent years. For instance, the 525 reported medical or healthcare data breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[26]

61. According to the U.S. Department for Health and Human Services' "2022 Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead," "[h]ealthcare data breaches have doubled in 3 years."[27]

62. PHI is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web.

---

[24] *Id*., pg. 6.
[25] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last accessed Apr. 14, 2023).
[26] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 7, 2022), at pg. 15.
[27] U.S. Department for Health and Human Services, The Health Sector Cybersecurity Coordination Center (HC3), "2022 Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead," February 9, 2023, avail. at https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf

63. PHI can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and medical records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

64. Given the nature of the Data Breach, it was foreseeable that the compromised PHI could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess the Class Members' PHI can easily obtain Class Members' tax returns or open fraudulent credit card accounts in the Class Members' names.

D. Defendants Failed to Comply with FTC Guidelines

65. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

66. In 2016, the FTC updated its publication, *Protecting PHI: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PHI that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[28]

[28] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for

67. The FTC further recommends that companies not maintain PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[29]

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. These FTC enforcement actions include actions against entities failing to safeguard PHI such as Defendants. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

70. M&D failed to properly implement basic data security practices widely known throughout the industry, and Island Ambulatory failed to ensure that its business associate, M&D, implemented these practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).

[29] *See id.*

71. Defendants were at all times fully aware of their obligations to protect the Personal Information of its current and former patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

E. Defendants Fail to Comply with Industry Standards

72. As shown above, experts studying cyber security routinely identify organizations holding PHI as being particularly vulnerable to cyber-attacks because of the value of the information they collect and maintain. As of 2022, ransomware breaches like that which occurred here had grown by 41% in the last year and cost on average $4.54 million dollars.[30]

73. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[31]

74. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

[30] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last accessed Apr. 14, 2023).
[31] *See* https://www.rapid7.com/solutions/compliance/critical-controls/ (last accessed Apr. 14, 2023).

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[32]

75. Upon information and belief, M&D failed to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and other industry standards for protecting Plaintiff's and the proposed Class Members' Personal Information—and Island Ambulatory failed to ensure that M&D met those standards—resulting in the Data Breach.

F. The Data Breach Caused Plaintiff and the Class Members Injury and Damages

76. Plaintiff and members of the proposed Class have suffered injury and damages from the unauthorized disclosure of their Personal Information in the Data Breach that can be directly traced to M&D's failure to adequately protect that Personal Information, and Island Ambulatory's

[32] Understanding The NIST Cybersecurity Framework, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Apr. 14, 2023).

failures to ensure M&D adequately protected that Personal Information, that has occurred, is ongoing, and/or imminently will occur.

77. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access the Plaintiff's and the proposed Class Members' Personal Information, which on information and belief is now being used or will imminently be used for fraudulent purposes and/or has been sold for such purposes and posted on the dark web for sale, causing widespread injury and damages.

78. The ramifications of Defendants' failure to keep Plaintiff's and the Class's Personal Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

79. Because Defendants collectively failed to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class Members have suffered, are at an increased risk of suffering, or will imminently suffer:

a. exposure of that Personal Information, including said information being posted on the Dark Web for fraudulent, criminal activity or sale;

b. fraudulent misuse of Personal Information, including fraudulent loans taken out using Personal Information acquired in the Data Breach, fraudulent cellular telephone accounts taken out using Personal Information acquired in the Data Breach; and, identity theft and impersonation using Personal Information acquired in the Data Breach;

c. Malware, and increase in spam emails;

d. The loss of the opportunity to control how Personal Information is used;

e. The diminution in value of their Personal Information;

f. The compromise and continuing publication of their Personal Information;

g. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

h. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

i. Emotional Distress;

j. Delay in receipt of tax refund monies;

k. Unauthorized use of stolen Personal Information; and

l. The continued risk to their Personal Information, which remains in the possession of Defendants and is subject to further breaches so long as M&D fails to undertake the appropriate measures to protect the Personal Information in its possession, and Island Ambulatory to ensure M&D undertakes these measures.

80. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

81. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts;

time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[33]

94. The FTC recommends that identity theft victims take several costly steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.[34]

95. The time-consuming process recommended by the FTC and other experts is complicated by the vulnerable situations of Defendants' patients.

96. Identity thieves use stolen Personal Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

97. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

---

[33] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last accessed Feb. 27, 2023).

[34] *See* https://www.identitytheft.gov/Steps (last accessed September 1, 2021).

98. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's Personal Information to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

99. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated. [35]

100. What's more, theft of Personal Information is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, Personal Information is a valuable property right.[36]

102. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that

---

[35] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last accessed Feb. 27, 2023).

[36] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

PHI has considerable market value.

103. Theft of Personal Information, in particular, is problematic because: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[37]

104. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed Personal Information to adjust their insureds' medical insurance premiums.

105. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when Personal Information and/or financial information is stolen and when it is used.

106. Personal Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

107. Where the most Personal Information belonging to Plaintiff and Class Members was accessible from M&D's network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

108. Thus, Plaintiff and the Class Members must vigilantly monitor their financial and

[37] *See Medical Identity Theft, Federal Trade Commission Consumer Information* (last visited: June 7, 2022), http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

medical accounts for many years to come.

109. According to cybersecurity experts, "[r]eports show the value of a health record can be worth as much as $1,000, whereas on the dark web, a credit card number is worth $5 and Social Security numbers are worth $1."[38]

110. Social Security numbers are among the worst kind of PHI to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[39]

111. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[40] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

112. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and

---

[38] Sanjay Cherian, Forbes Magazine, "Healthcare Data: The Perfect Storm," January 14, 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=28523ee56c88 (last accessed June 19, 2023).

[39] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Feb. 25, 2023)

[40] *See id.*

evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[41]

113. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[42] Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 per person and up.[43]

114. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the imminent identity fraud and criminal fraudulent activity; lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

115. Defendants knew or should have known of these harms which would be caused by the Data Breach they permitted to occur, and M&D should have strengthened its data systems accordingly, and Island Ambulatory should have ensured that M&D did so before entrusting Plaintiff's and the Class Members' Personal Information to M&D.

---

[41] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed September 1, 2021).

[42] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed September 1, 2021).

[43] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last accessed September 1, 2021).

CLASS ACTION ALLEGATIONS

116. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated (the"Class"):

> **All persons identified by Defendants (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

117. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

118. Plaintiff reserves the right to amend or modify the Class definitions as this case progresses.

119. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

120. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. if Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personal Information;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. if Defendant owed a duty to Class Members to safeguard their Personal Information;

f. if Defendant breached their duty to Class Members to safeguard their Personal Information;

g. if Defendant knew or should have known that their data security systems and monitoring processes were deficient;

h. if Defendant should have discovered the Data Breach sooner;

i. if Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. if Defendant's conduct was negligent;

k. if Defendant's breach implied contracts with Plaintiff and Class Members;

l. if Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. if Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. if Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

121. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data

Breach.

122. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

123. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

124. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

125. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

126. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. if Defendant failed to timely notify the public of the Data Breach;

b. if Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. if Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. if Defendant's failure to institute adequate protective security measures amounted to negligence;

e. if Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. if adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

127. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Proposed Class)

128. Plaintiff repeats and re-alleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

129. Plaintiff and the Class Members entrusted their Personal Information to Island Ambulatory, and other medical providers, who entrusted the Personal Information to M&D to perform medical billing services.

130. Defendants owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using the Personal Information in their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

131. Further, Defendants, Island Ambulatory and M&D owed to Plaintiff a duty to exercise reasonable care in supervising M&D to ensure M&D adequately protected the Personal Information which Island Ambulatory had entrusted to M&D.

132. Defendants owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendants' failure to collectively adequately safeguard the Personal Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Personal Information—just like the Data Breach that ultimately came to pass. Defendants Island Ambulatory and M&D acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's Personal Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the Personal Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

133. Defendants owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their Personal Information. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope,

nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

134. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants Island Ambulatory, and M&D knew or should have known would suffer injury-in-fact from said Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and members of the Class's Personal Information.

135. The risk that unauthorized persons would attempt to gain access to the Personal Information and misuse it was foreseeable. Given that Defendants holds vast amounts of Personal Information, it was inevitable that unauthorized individuals would attempt to access their databases containing the Personal Information—whether by a sophisticated cyberattack or otherwise.

136. Personal Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiff and Class Members and the importance of exercising reasonable care in handling it, and of Island Ambulatory in supervising M&D's handling of that information.

137. Defendants breached their duties by failing to exercise reasonable care in supervising its agents, employees, contractors, vendors, and suppliers, and in handling and securing the Personally Information of Plaintiff and Class Members, and by Island Ambulatory failing to ensure M&D did so, which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injury-in-fact and damages.

138. Defendants further breached their duties by failing to provide reasonably timely

notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

139. As a direct, proximate, and traceable result of Defendants' negligence, Plaintiff has suffered or will imminently suffer injury-in-fact and damages, as set forth in the preceding paragraphs.

140. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including: exposure of that Personal Information, including being posted on the Dark Web for fraudulent, criminal activity or sale; fraudulent misuse of Personal Information including fraudulent loans, fraudulent cellular telephone accounts, and identity theft and impersonation using Personal Information acquired in the Data Breach; malware, and increase in spam emails; loss of the opportunity to control how Personal Information is used; diminution in value of their Personal Information; compromise and continuing publication of their Personal Information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; emotional Distress; delay in receipt of tax refund monies; unauthorized use of stolen Personal Information; the continued risk to their Personal Information, which remains in the possession of Defendants and is subject to further breaches so long as M&D fails to undertake the appropriate measures to protect the Personal Information in its possession, and Island Ambulatory fails to ensure M&D undertakes these measures; and, an

increased risk of fraud and identity theft.

141. As a result of the negligence of Defendants, Plaintiff and the Class Members are entitled to recover actual, compensatory, and punitive damages.

142. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) properly notify affected victims of the Data Breach (ii) strengthen their data security systems and monitoring procedures; (iii) submit to future annual audits of those systems and monitoring procedures; and (iv) provide adequate credit monitoring to all Class Members.

143. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the Personal Information maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the exposure of the Personal Information of Plaintiff and the Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff Proposed Class)

144. Plaintiff repeats and re-alleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

145. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's Personal Information.

146. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers or, in this case, patients'

PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff's and the members of the Class's sensitive PII.

147. Defendants violated their respective duties under Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Plaintiff's and the Class's Personal Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to patients in the event of a breach, which ultimately came to pass.

148. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

149. Defendants had a duty to Plaintiff and the Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's Personal Information, and Island Ambulatory had the duty to supervise its service provider, M&D, to ensure it did so.

150. Defendants breached their respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's Personal Information.

151. Defendants' violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations including HIPAA constitutes negligence *per se*.

152. But-for Defendants' wrongful and negligent breach of its duties owed to Plaintiff

and members of the Class, Plaintiff and members of the Class would not have been injured.

153. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Personal Information.

154. Had Plaintiff and members of the Class known that Defendants did not adequately protect their Personal Information, Plaintiff and members of the Class would not have entrusted Defendants with their Personal Information.

155. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and members of the Class have suffered actual, tangible, injury-in-fact and damages, including: exposure of that Personal Information, including being posted on the Dark Web for fraudulent, criminal activity or sale; fraudulent misuse of Personal Information including fraudulent loans, fraudulent cellular telephone accounts, and identity theft and impersonation using Personal Information acquired in the Data Breach; malware, and increase in spam emails; loss of the opportunity to control how Personal Information is used; diminution in value of their Personal Information; compromise and continuing publication of their Personal Information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; emotional distress; delay in receipt of tax refund monies; unauthorized use of stolen Personal Information; the continued risk to their Personal Information, which remains in

the possession of Defendants and is subject to further breaches so long as M&D fails to undertake the appropriate measures to protect the Personal Information in its possession, and Island Ambulatory fails to ensure M&D undertakes these measures; and, an increased risk of fraud and identity theft.

156. As a result of the negligence *per se* of Defendants, Plaintiff and the Class Members are entitled to recover actual, compensatory, and punitive damages.

COUNT III
BREACH OF AN IMPLIED CONTRACT
(On Behalf of Plaintiff and the Proposed Class)

157. Plaintiff repeats and re-alleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

158. Defendant Island Ambulatory offered to provide medical services to Plaintiff and the Class Members in exchange for their Personal Information and in exchange for amounts paid for medical treatment and services that included payment for data security.

159. Island Ambulatory entrusted the Personal Information of Plaintiff and the proposed Class Members to M&D, their business associate, in order for M&D to perform medical billing services.

160. Plaintiff and the Class Members accepted Defendant Island Ambulatory's offer by providing Personal Information to Island Ambulatory, and in turn to M&D, in exchange for medical services.

161. In turn, and through internal policies described in the preceding paragraphs, and other conduct and representations, Defendants agreed they would not disclose the Personal Information they collect to unauthorized persons and that they would safeguard patient Personal Information, including by Personal Information supervising their business associate, M&D, to

ensure it adequately safeguarded patient Personal Information.

162. Implicit in the parties' agreement was that Defendants would provide Plaintiff and the Class Members with prompt and adequate notice of all unauthorized access and/or theft of their Personal Information.

163. Plaintiff and the Class Members would not have entrusted their Personal Information to Defendants in the absence of such an agreement with Island Ambulatory, and M&D.

164. Defendants materially breached the contract(s) each had entered into with Plaintiff and the Class Members by failing to safeguard their Personal Information, including by Island Ambulatory failing to supervise M&D to ensure it properly safeguarded their Personal Information, and by failing to notify them promptly of the Data Breach to M&D's computer systems that compromised such information. Island Ambulatory further breached the implied contracts with Plaintiff and the Class Members by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's Personal Information, including Island Ambulatory failing to properly supervise M&D to ensure it safeguarded the Personal Information entrusted to it;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic Personal Information that Defendants created, received, maintained, and transmitted.

165. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendants' material breaches of its agreement(s).

166. Plaintiff and the Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendants.

167. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

168. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

169. Defendants failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

170. In these and other ways, Defendants violated their duties of good faith and fair dealing.

171. Plaintiff and the Class Members have sustained injury-in-fact and damages because of Defendants' breaches of their agreements, including breaches thereof through violations of the covenant of good faith and fair dealing.

172. As a direct and proximate result of Defendants' breach of implied contract, Plaintiff and the proposed Class Members and are entitled to actual, compensatory, and consequential damages.

COUNT IV
THIRD-PARTY BENEFICIARY
(On Behalf of Plaintiff and the Proposed Class)

173. Plaintiff repeats and re-alleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

174. Plaintiff and the proposed Class Members are third-party beneficiaries of contracts between M&D and Island Ambulatory, and likely between M&D and other medical providers, under which M&D: received Plaintiff's and the Class's Personal Information; stored that information in its computer network systems; and provided medical billing and revenue cycle management services to their medical service providers.

175. Plaintiff and the proposed Class Members, as patients of Island Ambulatory or other parties in contract with M&D, were the intended beneficiaries of these contracts, in that the contracts all related to the provision of medical services to Plaintiff and the Class.

176. Defendants have breached the foregoing contracts by failing to adequately protect Plaintiff's and the Class Members' Personal Information, resulting in the Data Breach, and injury-in-fact and damages.

177. Defendants each materially breached the contract(s) each had entered into by failing to safeguard the Personal Information entrusted to it, including by Island Ambulatory failing to properly supervise M&D to endure it safeguarded Plaintiff's and the Class's Personal Information, and including breaches of the covenant of good faith and fair dealing.

178. As a direct and proximate result, Plaintiff and Class Members are entitled to actual, compensatory, and consequential damages.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Proposed Class)

179. Plaintiff repeats and re-alleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

180. This claim is pleaded as the alternative to the breach of implied contractual duty claim.

181. Plaintiff and the Class Members conferred a benefit upon Defendants in the form of monies paid for medical treatment services and by providing their Personal Information to Defendants in order to receive such services.

182. Defendants appreciated or had knowledge of the benefits conferred upon themselves by Plaintiff and the Class Members.

183. As a result of Defendants' conduct, Plaintiff and members of the Class suffered actual damages in an amount equal to the difference in value between the purchases made with reasonable data privacy and security practices and procedures that Plaintiff and the Class Members paid for, and the purchases without unreasonable data privacy and security practices and procedures that they received.

184. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and the proposed Class Members' payments and their Personal Information because Defendants failed to adequately protect their Personal Information, and because Island Ambulatory failed to properly supervise M&D to ensure it protected Plaintiff's and the Class Members' Personal Information. Plaintiff and the Class Members would not have provided their Personal Information, nor used and paid for Defendants' services, had they known Defendants would not adequately protect their Personal Information.

185. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach alleged herein.

COUNT V
INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS
(On Behalf of Plaintiff and the Proposed Class)

186. Plaintiff repeats and re-alleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

187. The Plaintiff and the Class Members took reasonable and appropriate steps to keep their Personal Information confidential from the public.

188. Plaintiff and the Class Members' efforts to safeguard their own Personal Information were successful, as their Personal Information was not known to the general public prior to the Data Breach.

189. Plaintiff and the Class Members had a legitimate expectation of privacy to their Personal Information, entrusted solely to Island Ambulatory for purpose of receiving medical treatment, which Island Ambulatory disclosed to M&D to perform medical billing services; and Plaintiff and the Class were entitled to the protection of this information against disclosure to unauthorized third parties.

190. Defendants owed a duty to Plaintiff and the Class Members to keep their Personal Information confidential.

191. The unauthorized release of Personal Information by Defendants in the Data Breach is highly offensive to a reasonable person.

192. Plaintiff and the Class Members' Personal Information is not of legitimate concern to the public.

193. Defendants knew or should have known that Plaintiff and Class Members' Personal Information was private, confidential, and should not be disclosed.

194. Defendants publicized Plaintiff and members of the Class's Personal Information, by unauthorizedly disclosing it to cyber criminals who had no legitimate interest in this Personal Information and who had the express purpose of monetizing that information through fraudulent misuse and by injecting it into the illicit stream of commerce flowing through the Dark Web.

195. Indeed, not only is Plaintiff and members of the Class's Personal Information published on the Dark Web, but upon information and belief, it is being used to commit fraud; it is being disseminated amongst, *inter alia,* financial institutions, merchants, creditors, health care providers and governmental agencies.

196. It is therefore substantially certain that the Plaintiff and the Class Members' Personal Information is rapidly becoming public knowledge—among the community at large—due to the nature of the cyber-attack that procured it, and the identity theft for which it is designed.

197. As a direct and proximate result of the invasion of privacy, public disclosure of private facts committed by Defendants, Plaintiff and the members of the Class have suffered injury-in-fact and damages as set forth in the preceding paragraphs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated individually, requests that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing Plaintiff's counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory,

actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: March 28, 2024

Respectfully submitted,

/s/Andrew J. Shamis
Andrew J. Shamis
Leanna A. Loginov
SHAMIS & GENTILE P.A.
14 NE 1st Avenue, Suite 705
Miami, Florida 33132
ashamis@shamisgentile.com
lloginov@shamisgentile.com

Counsel for Plaintiff and the Proposed Class